



# NASA Procedural Requirements

**COMPLIANCE IS MANDATORY**

**NPR 2841.1**

Effective Date: January 06,  
2011

Expiration Date: January 06,  
2016

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

---

## Identity, Credential, and Access Management

**Responsible Office: Office of the Chief Information Officer**

## Table of Contents

### Preface

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents
- P.5 Measurement/Verification
- P.6 Cancellation

### Chapter 1. Description of Services

- 1.1 Identity Management
- 1.2 Credential Management
- 1.3 Access Management

### Chapter 2. Responsibility

- 2.1 Agency Chief Information Officer
- 2.2 Agency Associate Administrator for Protective Services
- 2.3 ICAM Business Process Leads
- 2.4 ICAM Service Managers

### Chapter 3. Requirements

- 3.1 ICAM Service Managers
- 3.2 Center Security Office Personnel
- 3.3 Registration Authorities
- 3.4 Identity Sponsors
- 3.5 Access Sponsors

- 3.6 Information System Owners
- 3.7 Information Owners
- 3.8 Physical Asset Owners
- 3.9 Community Managers
- 3.10 Systems and Applications
- 3.11 Legacy and Special Purpose ICAM Service Providers
- 3.12 Federated Identity Providers and Credential Service Providers
- 3.13 End Users

## **Appendix A. Definitions**

## **Appendix B. Acronyms**

## **Appendix C. Additional References**

# Preface

## P.1 Purpose

This document establishes requirements and responsibilities for the policy set forth in NASA Policy Directive (NPD) 2800.1, Managing Information Technology, in order to properly manage identity, credential, and access management (ICAM) services as an integrated end-to-end service to improve security, efficiency, and inter-Center collaboration. In order to meet Federal requirements established by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST), and documented in the Federal ICAM Roadmap and Implementation Guidance, this NASA Procedural Requirement (NPR) establishes Agency-wide enterprise services that all Centers and applications shall use.

## P.2 Applicability

This NASA Procedural Requirement (NPR) is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to the Jet Propulsion Laboratory (JPL), other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

## P.3 Authority

- a. NPD 2800.1, Managing Information Technology.
- b. NPD 2810.1, NASA Information Security Policy.
- c. NPR 1600.1, NASA Security Program Procedural Requirements.
- d. NPD 2190.1, NASA Export Control Program.

## P.4 Applicable Documents

- a. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Electronic Authentication Guideline.
- b. NIST SP 800-82, DRAFT Guide to Industrial Control Systems (ICS) Security.
- c. x.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework.
- d. Personal Identity Verification Interoperability For Non-Federal Issuers.
- e. IT-HBK-2841-001, Identity, Credential, and Access Management (ICAM) Services Handbook.
- f. IT-SOP-2841-001, Identity Providers and Credential Service Providers Standard Operating Procedure (SOP).
- g. IT-SOP-2841-002, ICAM Services Deviation SOP.

## P.5 Measurement/Verification

Two measurements used to determine compliance with this NPR are:

- a. Are assets properly registered in the asset registration system (ref. 3.6.a)? To determine Center compliance with this NPR, the Office of the Chief Information Officer (OCIO) compares the asset registry with Information Technology (IT) System Security Plans, Internet Protocol (IP) address registrations, and other sources of asset data.
- b. Are assets properly utilizing Agency identities, credentials, and access management services? To determine Center compliance with this NPR, OCIO reviews reports from the asset registration system, IT System Security Plans, and information from ICAM services.

## **P.6 Cancellation.**

None.

/S/

Linda Y. Cureton  
Chief Information Officer

# Chapter 1. Description of Identity, Credential, and Access Management Services

1.1 Identity management services support identity life-cycle management, identity maintenance, and directory services as described below.

1.1.1 Identity life-cycle management services ensure that people are properly vetted based on their affiliation with NASA and the NASA facilities and systems to which they require access.

1.1.1.1 Identity life-cycle management services provide the ability to create, modify, vet, and retire the identities of people who access NASA facilities and systems.

1.1.1.2 Identity life-cycle management services provide a Level of Confidence (LoC) in a person's identity that can be measured against the Level of Risk (LoR) of access to a physical or logical asset.

1.1.1.3 Identity life-cycle management includes the management of federated identities from trusted identity providers both within and outside the Federal Government.

1.1.2 Identity maintenance services ensure that people can be found in NASA directories to support the conduct of NASA business.

1.1.2.1 Identity maintenance services provide the capability for people to change information about themselves. Examples include nicknames, display names, and NASA location information.

1.1.3 Directory services allow persons and non-person entities (NPEs) to search and retrieve information about people affiliated with NASA.

1.1.3.1 Directories leverage data from identity management and maintenance services discussed in Sections [1.1.1](#) and [1.1.2](#).

1.2 Credential management services support credential life-cycle management and certificate management as described below.

1.2.1 Credential life-cycle management services ensure that Agency credentials are issued, re-issued, suspended, or revoked based on affiliation and LoC information provided by authoritative identity management services.

1.2.1.1 Credential life-cycle management services also ensure that Agency credentials are issued using business processes that provide the required Level of Assurance (LoA) defined for the credential by NASA in the ICAM Services Handbook, based on NIST SP 800-63, Electronic Authentication Guidance [800-63].

1.2.1.2 Credentials are issued to allow access to both physical and logical assets throughout NASA.

1.2.2 Certificate management services ensure that Public Key Infrastructure (PKI) certificates for authentication, encryption, and signing operations are issued and maintained in accordance with the x.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework.

1.2.3 Certificate management services ensure that PKI certificates are issued, re-issued, suspended, and revoked based on affiliation and LoC information provided by authoritative identity management services.

1.2.3.1 Certificate management services provide PKI certificates for both persons and NPEs.

1.3 Access management services support asset management, community management, permission management, and authentication and authorization services for both physical and logical (IT) access, as described below.

1.3.1 Asset management services are provided to ensure the proper identification and registration of NASA's assets and the attributes needed for access management.

1.3.2 Community management services support the creation, modification, suspension, and disablement of communities of people who require access to assets or asset groups.

1.3.3 Permission management services ensure that access is granted to assets as required for a person to fulfill his or her assignment.

1.3.3.1 Approval-based permission services allow people to request access to NASA assets for themselves or others.

1.3.3.2 Basic Levels of Entitlement (BLEs) allow access to be granted to people based on communities and other attributes maintained in the Agency's identity management service. Access may be granted based on a person's relationship with NASA (e.g., civil servant, contractor, partner); discipline (e.g., scientist, engineer), or affiliation with a particular NASA organization.

1.3.4 Authentication services ensure that the person or NPE attempting to access an asset matches an asserted identity at the appropriate LoA.

1.3.4.1 Person-based authentication services ensure that persons attempting to access a NASA facility or system is who they claim to be at the appropriate LoA.

1.3.4.2 NPE authentication services validate that the NPE accessing the NASA IT infrastructure is a trusted entity.

1.3.5 Authorization services ensure that the person or NPE attempting to access the asset has a right to do so.

1.3.6 The Certificate Validation Service (CVS) is the authoritative source of valid PKI certificates.

1.3.6.1 The CVS provides status of revocation and expiration of previously issued PKI certificates.

1.3.6.2 The CVS is updated in near real time to increase the confidence that a person or NPE accessing a NASA asset is still eligible for the attempted access.

## Chapter 2. Responsibility

2.1 The Agency Chief Information Officer (CIO) has overall responsibility for implementation of the requirements outlined in this directive.

2.1.1 The Agency CIO shall ensure that ICAM services for accessing IT resources are implemented in compliance with applicable laws, regulations, and NASA program directives and requirements.

2.1.2 The Agency CIO shall maintain the ICAM Enterprise Architecture segment.

2.1.3 The Agency CIO shall publish and maintain the ICAM Services Handbook, which will provide detailed information and guidance about the use of systems and processes to meet the requirements in this NPR.

2.1.4 The Agency CIO, in coordination with the Agency Associate Administrator (AA) for Protective Services, shall select and support the ICAM Business Process Leads (BPLs) as described in Section [2.3](#).

2.2 The Agency AA for Protective Services shall ensure that ICAM services for accessing physical resources are implemented in compliance with applicable laws, regulations, and NASA program directives and requirements.

2.2.1 The Agency AA for Protective Services, in coordination with the Agency CIO, shall select and support the ICAM BPLs as described in Section [2.3](#).

2.3 The ICAM BPLs shall provide business requirements and manage implementation of ICAM services within their respective Centers or Mission Directorates.

2.3.1 The ICAM Center BPL (CBPL) shall provide overall coordination and management of ICAM business processes and implementation within their Centers or Mission Directorates. The ICAM CBPL is the liaison between Center/Mission Directorate operational components and Agency ICAM representatives for all ICAM activities and is the primary interface for Center-based outreach and communications related to ICAM services.

2.3.2 The Identity Management BPL shall provide the business requirements and business processes related to identity management processes, including processes for onboarding, transferring, and offboarding civil servants, contractors, and other affiliates whose association with NASA is permanent, temporary, or through remote IT access only.

2.3.3 The Credential Management BPL shall provide the business requirements and business processes related to credential management services, including but not limited to those related to issuance of the Federal Personal Identity Verification (PIV) smartcard credential, other smartcard credentials, PKI certificates, onetime password tokens, and User IDs/passwords.

2.3.4 The Logical Access Management BPL shall provide the business requirements and processes relating to access management for IT assets. This includes asset management, permission management, and access control services. The Logical Access Management BPL is also responsible for ensuring that compliance deadlines for IT asset integration in accordance with this NPR and related documents are met.

2.3.5 The Physical Access Management BPL shall provide the business requirements and processes relating to access management for physical assets. This includes asset management, permission management, and access control services.

2.4 ICAM Service Managers shall implement and operate the ICAM enterprise architecture segment. The Service Managers shall provide system designs, technical implementation, and operational support based on the business requirements and processes as defined by the ICAM BPLs and approved by the Agency CIO and the Agency AA for Protective Services.



# Chapter 3. ICAM Requirements

## 3.1 Identity, Credential, and Access Management (ICAM) Service Managers shall:

- a. Implement ICAM services in compliance with all Federal and NASA regulations.
- b. Implement ICAM services in alignment with NASA's ICAM Enterprise Architecture segment.
- c. Implement enhancements to ICAM services to meet customer requirements and requirements for integration with other NASA enterprise services as approved by the Agency CIO and the Agency AA for Protective Services.
- d. Be the sole provider of authoritative identity management and directory services.
- e. Be the primary provider of credential management and access management services.
- f. Accept trusted identities and/or credentials provided and managed by Federated Identity Providers (IdPs) and Credential Service Providers (CSPs), as needed, to support NASA's mission.

## 3.2 Center Security Office Personnel shall:

- a. Verify identities of persons who require access to NASA's physical and IT assets to meet the requirements of this NPR.
- b. Issue Agency credentials that are used for access to both physical and IT assets. The ICAM Services Handbook describes NASA-accepted credentials that can be used for both physical and logical access.
- c. Revoke Agency credentials when a person's affiliation with NASA has been terminated.
- d. Revoke Agency credentials as needed to address security threats.
- e. Accept trusted identities and/or credentials provided and managed by Federated IdPs or CSPs as needed to support NASA's mission.

## 3.3 Registration Authorities (RAs) shall:

- a. Issue credentials and certificates that are used solely for access to IT assets. The ICAM Services Handbook describes NASA-accepted credentials that can be used for logical access.
- b. Revoke credentials and certificates when a worker's affiliation with NASA has been terminated.
- c. Revoke credentials and certificates as needed to address IT security threats.

## 3.4 Identity Sponsors shall:

- a. Use the ICAM infrastructure for the creation and maintenance of identity information for all persons accessing NASA assets.
- b. Request identity disablement for persons who no longer have an active relationship with NASA.
- c. Request the acceptance of federated identities and/or credentials in accordance with the Identity Providers and Credential Service Providers SOP.

## 3.5 Access Sponsors shall:

- a. Validate an End User's need for access whenever a request for access is made.

- b. Request removal of access when an End User no longer requires access to perform his/her duties.
- c. Perform disposition of records as needed when an End User's access is terminated.

### 3.6 Information System Owners shall:

- a. Register their IT assets in the authoritative system of record for IT assets defined in the ICAM Services Handbook ensuring that:

(1) New assets are registered at the first stage of their construction or system development life cycle, generally prior to Preliminary Design Review.

(2) Existing assets are registered and maintained throughout their life cycle, culminating with asset retirement and decommissioning.

- b. Collaborate with the Information Owner(s) to ensure that an LoR is assigned to each type of access and/or access role for each IT asset under their System Security Plan(s).

- c. Collaborate with the Information Owner(s) to implement the appropriate provisioning method for managing access to their assets using the NASA access management service. One of the following methods may be used:

(1) An approval-based method for granting access to their IT asset(s).

(2) A BLE related to a community designation or other attributes maintained authoritatively in enterprise directory services.

- d. Ensure that all persons accessing their IT assets have a NASA-accepted identity.

- e. Ensure that persons granted access to their IT assets meet the appropriate LoC for the associated LoR of the access to the IT asset.

- f. Ensure that credentials allowed to access their IT assets meet the appropriate LoA for the associated LoR of the access to the IT asset.

- g. Reconcile all accounts recorded in the access management service with the accounts on the IT asset, ensuring that:

(1) Discrepancies between the account list in the access management service and the account list in the IT asset are analyzed and reconciled so that the access management service accurately reflects approved access to the asset.

(2) Reconciliation is conducted on an annual basis at a minimum.

- h. Request a deviation using the process described in the ICAM Services Deviation SOP to allow continued use of a legacy or special purpose ICAM service provider provided that:

(1) There is a technological constraint that does not allow the use of the NASA enterprise ICAM services.

(2) The legacy or special purpose ICAM service provider has met the requirements in Section [3.11](#) of this NPR.

(3) A transition plan is provided that details when the asset will be retired or integrated with the enterprise ICAM service.

- i. Delegate requirements in this NPR as appropriate to persons responsible for managing, operating,

and/or maintaining IT assets governed by their IT System Security Plan(s).

### 3.7 Information Owners shall:

- a. Assign an LoR to each type of access and/or access role (e.g., generation, collection, processing, dissemination, and disposal) for information under their authority.
- b. Collaborate with the Information System Owner to ensure that the credentials allowed to access information under their authority meets the appropriate LoA for the associated LoR of the access to the information.
- c. Determine the appropriate provisioning method to manage access to information under their authority, utilizing the NASA access management service using one of the following methods:

(1) An approval-based method for granting access to their IT asset(s).

(2) A BLE related to a community designation or other attributes maintained authoritatively in enterprise directory services.

### 3.8 Physical Asset Owners shall:

- a. Ensure that their physical assets have been properly registered in the authoritative system of record for physical assets defined in the ICAM Services Handbook.
- b. Assign a LoR to each type of access for each physical asset.
- c. Manage access to their physical assets using the NASA access management service using one of the following methods:

(1) An approval-based method for granting access to their asset.

(2) A BLE related to a community designation or other attributes maintained authoritatively in enterprise directory services.

- d. Ensure that all persons accessing their physical assets have a NASA-accepted identity.
- e. Ensure that persons have been verified to the appropriate LoC to meet the associated LoR of their access to the physical asset.
- f. Ensure that credentials allowed to access their physical assets meet the appropriate LoA for the associated LoR of the access to the physical asset.

### 3.9 Community Managers shall:

- a. Manage membership in their communities within the access management service using one of the following methods:

(1) An approval-based method.

(2) A logical combination of other communities or attributes maintained authoritatively by identity management services.

(3) Self-registry by the membership.

(4) A combination of self-registry, approval-based, and attribute-based methods.

- b. Approve BLE access of their communities to assets.

- c. Notify all asset owners who grant access to their community of any change to the membership

requirements of their community.

3.10 Systems and Applications shall be designed to:

- a. Utilize enterprise directory services for person lookup services provided by their systems.
- b. Utilize enterprise authentication and authorization services for end user authentication and authorization.

(1) Systems and applications may utilize internal authorization mechanisms for fine-grained, role-based authorization.

- c. Use Agency-accepted credentials for access to all NASA IT assets.
- d. Utilize NASA-accepted certificates for person and NPE authentication, encryption, and signing.

3.11 Legacy and special purpose ICAM service providers may continue to operate their services provided that:

- a. The legacy or special purpose service relies on identities maintained in the ICAM identity management service.
- b. There is a technological constraint that does not allow applications or systems utilizing the service to transition to the NASA enterprise ICAM services.
- c. A deviation request is submitted and approved in accordance with the ICAM Services Deviation SOP.
- d. Federal and NASA requirements for ICAM services are met.
- e. A transition plan is provided that details when the service will be retired or integrated with enterprise ICAM services.

3.12 Federated Identity Providers (IdPs) and Credential Service Providers (CSPs) shall:

- a. Apply for acceptance of their identities and/or credentials using ICAM Identity Providers and Credential Service Providers SOP.
- b. Conform to Federal interoperability standards.
- c. Conform to NASA interoperability standards.
- d. Be sponsored by a NASA civil servant in order for the request to be considered.

3.13 End Users shall:

- a. Notify their Identity Sponsor of any changes in identity information, such as legal name or citizenship status. For civil servants, the Identity Sponsor is the Office of Human Capital Management. For contractors, the Identity Sponsor is the Contracting Officer's Technical Representative (COTR).
- b. Use only the credential(s) issued to them for access to NASA assets.
- c. Not share their credentials and/or secret keys with another person.
- d. Secure their credentials and secret keys in a way that reduces the likelihood that they will be used by others.
- e. Ensure the validity of certificates provided by other parties in PKI encoded transactions and

sessions.

f. Upon notification, review access granted to them through the access management service, and request that access be rescinded for any asset they no longer require to perform assignments.

g. Upon notification, request that membership be rescinded for any community no longer required to perform assignments.

h. Sign and encrypt data in accordance with Federal and NASA regulations using only NASA-accepted encryption and signing certificates.

i. Encrypt data in accordance with Federal and NASA regulations using only NASA-accepted encryption tools.

# Appendix A. Definitions

- A.1 **Access.** The ability to (1) obtain and use information and related information processing services; and/or (2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).
- A.2 **Access Control.** The process of granting or denying specific access requests.
- A.3 **Access Sponsor.** A NASA person who can vouch for another individual's need for access to an asset.
- A.4 **Application.** (1) A set of computer commands, instructions, and procedures used to cause a computer to process a specific set of information. Application software does not include operating systems, generic utilities, or similar software that are normally referred to as "system software." (2) A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate that individual's interaction with the system.
- A.5 **Asserted Identity.** The set of attributes that an individual claims uniquely identifies him or her.
- A.6 **Asset.** A system, object, person, or any combination thereof, that has importance or value: includes facilities, property, information records, data, information technology systems, and applications.
- A.7 **Asset Group.** A collection of assets that are managed together for purposes of identifying Level of Risk (LoR), granting access permissions, and/or authorizing access.
- A.8 **Authentication.** (1) The validation and confirmation of a person's claim of identity. (2) The validation and identification of a computer network node, transmission, or message. (3) The process of establishing confidence of authenticity. (4) Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to facilities and information systems.
- A.9 **Authoritative.** A source of data or information that has been sanctioned by established authority as the best source of information that can be found within a given domain.
- A.10 **Authorization.** The privilege granted to a subject (e.g., individual, program, or process) by a designated official to do something, such as access information based on the individual's need to know.
- A.11 **Basic Level of Entitlement (BLE).** Access right(s) granted to a person based on attributes, including but not limited to affiliation, geographical location, and community membership.
- A.12 **Certificate.** See digital certificate.
- A.13 **Certificate Validation.** Transactions used to verify that a digital certificate is still valid, e.g., not revoked or expired.

- A.14 **Credential.** A physical/tangible or electronic object through which data elements associated with an individual are bound to the individual's identity. Credentials are presented to access control systems in order to gain access to assets.
- A.15 **Credential Service Provider (CSP).** An element of an authentication system which issues and performs life-cycle management of identity information and associated credentials.
- A.16 **Community Manager.** The individual responsible for the creation and management of a group of NASA people, generally for the provision of access to one or more assets. Members of communities have something in common that is encapsulated in an attribute of the person, including but not limited to affiliation, discipline, or organization.
- A.17 **Digital Certificate.** A credential in the form of encoded data which serves as a guarantee that parties to a transaction are who they claim to be.
- A.18 **Encryption.** Any procedure used in cryptography to convert plain text into cipher text in order to prevent anyone other than the intended recipient from reading that data.
- A.19 **End User.** A person who relies on computer systems to conduct duties or business activities.
- A.20 **Enterprise Architecture.** The organizing logic for business processes and Information Technology (IT) infrastructure reflecting the integration and standardization requirements of the firm's operating model.
- A.21 **Federated Identity.** The set of attributes of an individual that are provided to NASA and maintained by a trusted external organization to uniquely identify the individual for the purpose of gaining logical and physical access to protected resources.
- A.22 **Identity, Credential, and Access Management (ICAM) Service Managers.** ICAM Service Managers are funded and tasked to provide one or more ICAM Services to the NASA Enterprise.
- A.23 **Identity.** The set of attributes that uniquely identify an individual for the purpose of gaining logical and physical access to protected resources and identification in electronic transactions.
- A.24 **Identity Proofing.** The process for providing sufficient information (e.g., identity history, credentials, documents) to a Registration Authority (RA) when attempting to establish an identity or issue a credential.
- A.25 **Identity Provider (IdP).** An issuing authority that binds vetted claimed identities to credentials for the purpose of assertion in electronic transaction requiring authentication.
- A.26 **Identity Sponsor.** A NASA civil servant who vouches for an individual's need for identity life-cycle management services in order to be authorized to access NASA physical or IT assets.
- A.27 **Identity Verification.** The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the credential or system and associated with the identity being claimed.



- A.28 **Information Owner (IO).** A NASA official with the responsibility to categorize and classify data, and to establish security controls for the generation, collection, processing, dissemination, and disposal of information under their authority. IOs and Information System Owners (ISOs) are often the same person. See NPR 2810.1 for more details about IO roles and responsibilities.
- A.29 **Information System Owner (ISO).** The NASA official who is responsible for the successful operation and protection of the system and its information. Program, project, and functional managers are often identified as information system owners. IOs and ISOs are often the same person. See NPR 2810.1 for more details about ISO roles and responsibilities.
- A.30 **Information Technology.** (1) Hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether by computers, telecommunications systems, automatic data processing equipment, or other. (2) Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: i) requires the use of such equipment; or ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
- A.31 **Infrastructure.** A collection of assets. See definitions for asset and system.
- A.32 **Interoperability.** For the purposes of this standard, interoperability allows any Government facility or information system, regardless of the credential issuer, to verify a cardholder's identity.
- A.33 **Information Technology (IT) Asset.** A system, application, or information that is managed under a NASA IT System Security Plan.
- A.34 **Legacy.** A service, system, or application that was operational prior to the initial publication of this NPR.
- A.35 **Level of Assurance (LoA).** The amount of certainty that individuals accessing a physical or logical asset are who they claim to be. NIST SP 800-63 provides guidance for determining LoA.
- A.36 **Level of Confidence (LoC).** The amount of certainty, based on identity proofing and investigation, that an individual can be trusted with access to NASA physical and IT assets.
- A.37 **Level of Risk (LoR).** The amount of vulnerability to NASA, based on the likelihood and consequences of an adverse action through improper access or use of a physical or IT asset.
- A.38 **Logical Access.** Access to information records, data, information technology systems, and applications.



- A.39 **NASA-Accepted Identity.** An identity of a person that is affiliated with NASA or a NASA-accepted Identity Provider (IdP) that meets Federal requirements for the asserted LoC. NIST SP 800-63 provides guidance for LoC, which ranges from little or no confidence to very high confidence.
- A.40 **NASA-Accepted Credential.** A credential that has been issued by NASA or by a NASA-accepted Credential Service Provider (CSP), and meets Federal requirements for the asserted LoA.
- A.41 **Non-Person Entity (NPE).** A computer, device, system or application. In this document, an NPE may be issued credentials and or certificates in order to allow for secure transfer of data to another NPE.
- A.42 **Person.** A NASA worker or partner with whom NASA collaborates and conducts business.
- A.43 **Personal Identity Verification (PIV) Smartcard.** A physical artifact that meets the requirements of Federal Information Processing Standard (FIPS) 201-1 and supporting documents, issued to an individual so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
- A.44 **Physical Access.** Access to NASA facilities and property.
- A.45 **PIV Sponsor.** A NASA Civil Servant who can approve the request for a NASA PIV smartcard for a person.
- A.46 **Public Key Infrastructure (PKI).** A service that provides the cryptographic keys needed to perform identity verification, encryption, and electronic signature.
- A.47 **Registration Authority.** Registration Authorities ensure that credentials are issued to, and shared secrets are created by, the person to whom the credential is assigned.
- A.48 **Remote [End] User.** Non-NASA personnel gaining logical access to NASA information system and application resources.
- A.49 **Revocation.** The removal of an individual's eligibility to access physical or logical assets based upon an adjudication that continued access poses a risk to the Agency.
- A.50 **Signing Certificate.** Digital certificate issued by a certificate authority to ensure integrity and authenticity in electronic transactions between individuals.
- A.51 **Smartcard.** Credential issued with an individual's unique vetted identity information encoded and physically printed on the exterior.
- A.52 **Special Purpose.** Special Purpose refers to IT assets that are unique in design or implementation in order to meet NASA's mission.
- A.53 **Suspension.** The temporary cessation of affiliation, community membership, use of credentials, or access. In this document, suspensions result in a temporary loss of access to physical or logical assets.

- A.54 **System.** In this document, this term is used to mean an interconnected set of information resources under the same management control which shares common functionality and requires the same level of security controls. Normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people.
- A.55 **System Owner.** See IT System Owner.
- A.56 **User.** Individual or (system) process authorized to access an IT asset.
- A.57 **User Authentication.** A process by which a system receives validation of a user's identity.
- A.58 **User Identification (User ID).** A unique character string used in a computer to identify a user which is not normally protected as private/privileged information but is unique within the system.
- A.59 **Vetted.** See Vetting.
- A.60 **Vetting.** A review of information about a person for possible approval or acceptance. In this document, a vetted person has been reviewed to determine eligibility for access to NASA physical and/or logical assets.

# Appendix B. Acronyms

AIMO	Agency Information Management Official
BLE	Basic Level of Entitlement
BPL	Business Process Lead
CBPL	Center Business Process Lead
CIO	Chief Information Officer
CSP	Credential Service Provider
CVS	Certificate Validation Service
ICAM	Identity, Credential, and Access Management
ICS	Industrial Control System
ID	Identifier
IdP	Identity Provider
IP	Internet Protocol
IT	Information Technology
FIPS	Federal Information Processing Standard
JPL	Jet Propulsion Laboratory
LoA	Level of Assurance
LoC	Level of Confidence
LoR	Level of Risk
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPE	Non-person Entity
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
PIV	Personal Identity Verification
RA	Registration Authority

SOP	Standard Operating Procedure
SP	Special Publication
STD	Standard

# Appendix C. Additional References

- C.1 Federal Information Security Management (FISMA) Act of 2002.
- C.2 OMB Memo M-04-04, E-Authentication Guidance for Federal Agencies.
- C.3 OMB Memo M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 -- Policy for a Common Identification Standard for Federal Employees and Contractors.
- C.4 OMB Memo M-06-16, Protection of Sensitive Agency Information.
- C.5 OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
- C.6 Federal Information Processing Standards (FIPS) 201, Personal Identity Verification of Federal Employees and Contractors.
- C.7 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, Risk Management Guide for Information Technology Systems.
- C.8 NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations.
- C.9 NIST SP 800-63, Electronic Authentication Guideline.
- C.10 NIST SP 800-82, DRAFT Guide to Industrial Control Systems (ICS) Security.
- C.11 NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
- C.12 x.509 Certificate Policy For The U.S. Federal PKI Common Policy Framework.
- C.13 Federal Identity, Credentialing, and Access Management Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3.
- C.14 Personal Identity Verification Interoperability For Non-Federal Issuers.
- C.15 NPR 2810.1, Security of Information Technology.
- C.16 NPR 2190.1, NASA Export Control Program.
- C.17 NASA STD 2804, Minimum Interoperability Software Suite.
- C.18 NASA STD 2805, Minimum Hardware Configurations.
- C.19 IT-HBK-2841-001, Identity, Credential, and Access Management (ICAM) Services Handbook.
- C.20 IT-SOP-2841-001, Identity Providers and Credential Service Providers SOP.
- C.21 IT-SOP-2841-002, ICAM Services Deviation SOP.